Department of the Army ***TRADOC Regulation 25-70**
Headquarters, United States Army
Training and Doctrine Command
Fort Monroe, Virginia 23651-1047

12 October 2004

Information Management: Automation

NETWORK SERVICES

Summary. This regulation establishes commandwide policy for managing, operating, and using network services, primarily electronic mail and the World Wide Web. It includes general policies for authorized uses and protection of information accessible via the Internet.

Applicability. This regulation applies to all U.S. Army Training and Doctrine Command (TRADOC) managers, operators, and users of network services.

Supplementation. Supplementation is authorized as required to amplify local policy for the management, operation, and use of network services. Forward one copy of supplement to Commander, TRADOC (ATIM-T), 84 Patch Road, Fort Monroe, VA 23651-1051, within 10 days of publishing.

Suggested improvements. The proponent of this regulation is the Chief Information Officer. Send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) through channels to Commander, TRADOC (ATIM-T), 84 Patch Road, Fort Monroe, VA 23651-1051. Suggested improvements may also be submitted using DA Form 1045 (Army Ideas for Excellence Program (AIEP) Proposal).

Availability. This publication is available on the TRADOC Homepage at http://www.tradoc.army.mil/tpubs/regndx.htm.

Summary of changes. This revision—

- Deletes responsibilities assigned to Directors of Information Management (DOIMs). Reassigns responsibilities remaining at TRADOC. Requires TRADOC activities coordinate service provision with their supporting garrison.
- Deletes guidance about networking infrastructure and system configurations DOIMs previously used in the execution of their responsibilities.

- Deletes previous TRADOC-specific guidance that is now issued at Army level, for example, personnel security procedures for network access.
- Establishes an Information Protection Working Group, chaired by HQ TRADOC Deputy Chief of Staff for Intelligence, to monitor the security of information posted on networks.
- Updates user authentication measures for private network services.
- Adds responsibilities for Public Affairs Officers to review content for release on publicly accessible web sites.

Contents

---

1. Purpose. This regulation prescribes policy and assigns responsibilities within U.S. Army Training and Doctrine Command (TRADOC) for managing, operating, negotiating, and using network services. Primary network services are electronic mail (E-mail) and web sites. TRADOC's objective is the maximum availability of network services, at an acceptable level of risk, for the execution of official business. This regulation distinguishes policies for publicly and privately accessible services that give a persistent presence to information on the Internet—primarily web sites. Public web sites are accessible from the Internet and use no positive access control, for example, user authentication or firewalls, to restrict access to the information posted on the web site. Private web sites screen or challenge users prior to permitting access to the information posted on the site.

*** This regulation supersedes TRADOC Regulation 25-70, 7 July 2000.**

2. References. Appendix A contains required publications.

3. Explanation of abbreviations and terms. Abbreviations and special terms used in this regulation are explained in the glossary.

4. Responsibilities.

a. Headquarters (HQ) TRADOC, Chief Information Officer (CIO) will—

(1) Define and enforce policies, procedures, and technical standards, as required, to ensure commandwide interoperability and security of network services.

(2) Coordinate with Office of the Army CIO/G-6, Network Enterprise Technology Command, and the Installation Management Agency regarding implementation of information assurance procedures and tools for TRADOC's network services. Prescribe measures to control access, input, and use of network services.

(3) Provide strategic planning guidance to assist TRADOC organizations in the negotiation of agreements for delivery of network services by supporting Directors of Information Management (DOIMs) or other information technology (IT) providers.

(4) Serve as webmaster of the top level HQ TRADOC homepages.

b. Headquarters TRADOC Deputy Chief of Staff for Intelligence (DCSINT) will—

(1) Coordinate the development of policies and procedures for securing web-based controlled unclassified information.

(2) Establish and chair a permanent Information Protection Working Group (IPWG) to assist in policy, training, resourcing, assessing, and red teaming TRADOC security for network services.

(3) Provide threat, technical, and security support to TRADOC activities.

c. Headquarters TRADOC Public Affairs Officer (PAO) will—

(1) Coordinate the TRADOC corporate information content and major themes on the TRADOC homepage and pages linked off the TRADOC homepage.

(2) Coordinate with the TRADOC CIO on any content that may affect the supporting information technology or conformance with web site policies.

(3) Coordinate with the TRADOC Strategic Communications Office on information and themes to highlight on the TRADOC homepage.

(4) Approve for release new content posted on the TRADOC corporate web site. New content includes buttons, text links, or other elements that affect the TRADOC homepage design.

(5) Serve as TRADOC web content executor (Chief, PAO) and web content manager (Chief, Command Information Branch) for the TRADOC corporate web site.

d. TRADOC commanders, commandants, directors of major subordinate commands (MSC), centers, schools, and activities will—

(1) Enforce Army and TRADOC policies regarding the planning, management, operation, and use of network services by their assigned organizations.

(2) Assign responsibilities to execute Army and TRADOC policies for the planning, requirements definition, negotiation for delivery, management, operation, and use of network services. This regulation refers to the assigned individual(s) for a TRADOC MSC, center, school, or activity as an Information Management Officer (IMO).

(3) Oversee the development, negotiation, and execution of agreements with the supporting garrison commander, DOIM, and other IT service providers, for secure access to and administration of networks, servers, and common user software.

(4) Enforce Army, TRADOC, and local information assurance (IA) policies applicable to the management and use of network services.

(a) Implement IA system architecture mandates, system protection features, and procedural security measures to minimize the potential for fraud, misappropriation, unauthorized disclosure, loss of data, or misuse.

(b) Ensure accreditation of assigned networks, computers, peripherals, and devices in accordance with (IAW) Army Regulation (AR) 25-2, chapter 5.

(c) Assign responsibilities to manage secure use of network services IAW AR 25-2. Assigned personnel are referred to in this regulation as the IMO or, for specific systems, the Information Assurance Security Officer (IASO).

(5) Ensure information posted to public web sites is reviewed for public release consistent with Department of Defense (DOD), Army, TRADOC, and local command policies.

(6) Assign responsibilities to execute Army and TRADOC policies for the management of web sites. Assigned personnel are typically the IMO, the webmaster, and the web site content manager (see paras c(5) and d(2), above).

(7) Assign responsibilities to supporting PAO to serve as web site content manager, and in that capacity, approve for public release information for posting to the public web site.

e. Information Management Officers will—

(1) Plan and manage the provision of network services for their assigned organizations.

(2) Coordinate the provision of network services, IAW local support agreement(s), with the supporting DOIM. Manage the issuance of user identification and passwords for supported TRADOC personnel.

(3) Coordinate IA procedures and incident responses with the supporting Information Assurance Manager (IAM) and with all local TRADOC IASOs.

(4) Oversee the training of TRADOC general users regarding:

(a) The authorized use of network services.

(b) The protection of controlled unclassified information and the risk it poses to soldiers when released on the Internet.

f. Designated records coordinators and records custodians will monitor the application of records management procedures IAW AR 25-400-2 to electronic records.

g. Webmasters will—

(1) Maintain registration of all public homepages with the Government Information Locator Service and coordinate the establishment of new homepages with the TRADOC webmaster (webmaster@monroe.army.mil).

(2) Manage the periodic review of web sites for security risks and design deficiencies. Inform web site content managers about, and ensure quick resolution of, identified problems.

(3) Ensure assigned TRADOC organizations' web sites comply with current DOD and Army policy, which is found at http://www.army.mil/webmasters/. Establish local policy as required.

(4) Provide information about local operations as requested by the TRADOC CIO.

(5) Coordinate the resolution of deficiencies the HQ TRADOC IPWG, CIO, or local PAO or IMO identified on assigned web sites.

h. Public Affairs Officers at HQ and activity level will—

(1) Review materials prior to posting on a public web site. Ensure content provider has coordinated with local operations security (OPSEC) officer and, if needed, Staff Judge Advocate (SJA) for review prior to releasing information.

(2) Serve as web site content manager for the activity's public homepage and pages linking from the homepage.

(3) Establish local procedures, in coordination with local OPSEC officer, SJA, and webmaster, for review and clearance of information posted to the assigned TRADOC organization's web sites.

(4) Coordinate incorporation of TRADOC and local strategic communications themes into web site displays.

i. Staff Judge Advocates at HQ and activity level will review materials, per requests from commands, units, or organizations, prior to posting on a public web site.

j. General users will—

(1) Use government-provided access to network services for official business and authorized purposes only (see para 5, below).

(2) Ensure they do not process, post, or transmit classified information via unclassified networks. Ensure Army information made available on public web sites is first coordinated with the local OPSEC officer and PAO prior to public dissemination.

(3) Apply information security guidance in the transmission or posting of controlled unclassified information.

(4) Notify IMO or IASO of possible security compromises, virus contamination through file transfer/execution or E-mail, and forgotten passwords.

5. Authorized use. This paragraph provides commandwide policies concerning the authorized use of all network services.

a. TRADOC personnel will limit their use of government-provided network services to official business and authorized purposes. This includes use of government-provided services from the home or during off-duty hours, and specifically prohibits Internet access for unauthorized personal use. Inappropriate use of TRADOC network services may be a basis for disciplinary action and/or denial of network services for any user.

b. Authorized purposes can include personal communications that are reasonably made from the workplace, to include communications by E-mail and brief Internet searches, provided such use—

(1) Causes no adverse impact on the employee's official duties.

(2) Is of reasonable duration and during personal time (for example, before or after the workday, break periods, or lunch) as much as possible.

(3) Serves legitimate public interest (for example, enhancing employee proficiency in use of the system or enhancing professional skills).

(4) Causes no adverse reflection on DOD.

c. Authorized purposes also include professional development. Such use will not detract from primary duties and mission accomplishment.

d. Specific examples of these authorized purposes include, but are not limited to, sending E-mail to build office morale by keeping employees informed of office activities (for example, office parties or status of sick employees), sending E-mail to families at home while on temporary duty, making a medical appointment, reading a news magazine at a web site, browsing for professional information having general relevance to your official duties, searching for job announcements as a result of government downsizing, and subscribing to professional mail list servers. Authorized purposes will not include sending electronic chain letters or “for sale” messages, fundraising for private enterprises, or conducting a private business, such as a tax preparation service.

e. Department of Defense 5500.7-R (The Joint Ethics Regulation (JER)) specifically prohibits using government equipment for outside employment. Personal use means nongovernment activity that is conducted for purposes other than outside employment. Personal use also excludes using government office equipment for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include gambling, hate speech, sexually explicit materials, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation. The creation, downloading, storage, copying, transmission, or retransmission of chain letters, broadcast transmissions, or other mass mailings, regardless of the subject matter, is inappropriate use.

f. Any use that could cause congestion, delay, degradation, or disruption of service to any government system or equipment is inappropriate. For example: video, sound, or other large files, “push” technology on the Internet and other continuous data streams, and establishing a connection to an unofficial “chat room” or instant messaging client.

g. Mission commanders and supervisors may further restrict the scope of authorized purposes as required (for example, to relieve the burden on the local network system capabilities or costs, or further limit periods of the duty day during which time is spent on E-mail or the Internet in order to increase worker efficiency).

h. Use of TRADOC communications resources is not anonymous. In accordance with the JER (Sections 2-301.A (3) and (4)), use of network services, the Internet, E-mail, or any automated information system serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized.

i. Information Management Officers or IASOs will report possible occurrences of unauthorized use to the soldier/employee's immediate commander/supervisor, who will consider appropriate disciplinary or other corrective action.

6. Information assurance. This paragraph provides commandwide policies for protecting information made accessible through a network service, primarily web sites.

a. The following sources and types of information are considered essential elements of friendly information. Such information must not be made publicly accessible.

(1) Training support plans, mission training plans, drills, field manuals, tactical vignettes, and other material that describes how soldiers perform basic functions in the current environment the U.S. Army finds itself, is protected, at a minimum, with For Official Use Only (FOUO). Examples include small unit tactics patrolling, stability and support operations, engineer operations, aviation operations, logistics procedures, and systems capabilities.

(2) Specific vulnerabilities to operations, equipment, or personnel, including, but not limited to, force protection, significant troop movements, readiness data, and tactics, techniques, and procedures (TTP) are marked, at a minimum, with CONFIDENTIAL, unless a colonel or above determines that the information is adequately protected with a marking of FOUO. CONFIDENTIAL information is secured IAW AR 380-5, and will not be made accessible from any UNCLASSIFIED server or web site, to include private web sites.

(3) Lessons learned, formal and informal TTP, and "how-to" articles that deal with topics described in paragraphs (1) and (2) above.

(4) Chat rooms and forums, whether operated by TRADOC, TRADOC personnel, or in partnership with non-TRADOC organizations, where information regarding topics listed in paragraphs (1) and (2) above is exchanged.

(5) Press releases that detail how soldiers are accomplishing the mission.

(6) Information relating to the funding, fielding, vulnerabilities, and capabilities of new equipment.

b. Public Affairs Officers must clear information for posting on public web sites. When requested by PAOs, the OPSEC officer and SJAs will assist in information reviews. TRADOC personnel will not make accessible the following types of information using public web sites:

(1) Classified information.

(2) Privacy Act information.

(3) For Official Use Only information.

(4) Unclassified information that requires special handling, for example, Encrypt For Transmission Only, Limited Distribution, and scientific and technical information protected under the Technology Transfer Laws.

(5) Freedom of Information Act (FOIA) exempt information.

c. When TRADOC activities require web capabilities for controlled unclassified information, they will protect the content using private web sites, protected by one of the following three methods. Commanders will not permit the establishment or continued operation of private web sites that are not secured by one of these methods:

(1) Authenticate all users via Army Knowledge Online (AKO). Information Management Officers should coordinate with supporting DOIM and Office of the Army CIO/G-6, Chief Technology Office, to make sites accessible to selected members, based on selected AKO attributes. For example, AKO users with only guest accounts may be screened from access.

(2) Authenticate all users via another DOD or Army compiled database, for example, the Defense Enrollment Eligibility Reporting System.

(3) Implement local password protection. Coordinate implementation with the supporting DOIM.

d. Information Management Officers and IASOs will coordinate with supporting DOIM to ensure servers and operating system

software that host TRADOC-supported private web sites comply with policies in AR 25-2, paragraph 4-20, for system security, for example, secure sockets layer, public key encryption, and reverse proxy servers.

e. All users, IMOs, and IASOs of network services will report incidents with potential or demonstrated impact on information assurance (for example, denial of service attacks, receipt of virus transmissions, breach of passwords) IAW AR 25-2, chapter 4, section VIII. The reporting channel extends from the user, through their supporting IASO, to the IAM for the installation. Information Assurance Security Officers will ensure incidents reported to the Army Computer Emergency Response Team are also reported to the TRADOC CIO.

f. To protect against the spread of computer viruses through network services, TRADOC activities will comply with the supporting DOIM/IAM's virus checking software architecture and procedures.

g. All information posted to a public web site is considered a Federal record. Unless access to the web site can be restricted to appropriate users, TRADOC personnel will not post nonrecord material such as coordinating draft documents that contain raw data or controlled information.

h. Use of outbound file transfer protocol (FTP) services, with or without a World Wide Web (WWW) user interface, is permissible. Information Management Officers will coordinate with supporting DOIM/IAM for technical assistance to ensure the functional requirements can be met within IA constraints.

i. Policy regarding personnel security in AR 25-2 applies for accessing network services.

7. Electronic mail. This paragraph provides commandwide policies specific to managing, operating, and using E-mail services.

a. TRADOC activities will maximize the use of DOIM-provided E-mail services. Since E-mail is a common user service provided by DOIMs, TRADOC activities will not implement new E-mail servers without coordinating an exception to do so with TRADOC CIO. Activities will document local variations or extensions of Army Baseline Services for the provision of E-mail services, and any associated reimbursable costs, in a Service Level Agreement with the supporting garrison (that is, DOIM).

b. Commanders and activity heads will establish and enforce local procedures to minimize improper use of E-mail. Improper uses include:

(1) Exploiting list servers or similar group broadcast systems for purposes beyond their intended scope to widely distribute unsolicited E-mail.

(2) Sending the same E-mail message repeatedly to one or more recipients to interfere with the recipient's use of E-mail.

(3) Sending or broadcasting E-mail messages of quotations, jokes, etc., to multiple addressees.

(4) Sending or broadcasting unsubstantiated virus warnings from sources other than IAMs.

c. With the exception of users responsible for disseminating information organization-wide (for example, personnel officers, command group, IMOs), users will not broadcast to distribution lists for the installation, domain, server, or TRADOC school. Information Management Officers will advise users on proper use of distribution lists when specific instances of indiscriminate distribution are identified. Information Management Officers may rescind services if abuse continues.

d. Users will not conduct official business using privately acquired commercial E-mail accounts (for example, Hotmail, America Online, etc.). If E-mail access is required while away from the office (for example, while on temporary duty) and the office account is not accessible over the Internet, users will restrict official E-mail to their Army Knowledge Online (AKO) account. All TRADOC personnel who are authorized E-mail accounts are required to also have AKO Web mail. TRADOC personnel will not set their defaults on AKO Web mail to automatically forward E-mail to personal accounts on commercial E-mail services.

e. Information Management Officers will ensure the establishment of an organizational E-mail account, using office symbols, for each serviced office (no lower than division level) to receive official correspondence. Information Management Officers will coordinate with the supporting IAM regarding the application of current DOD and Army policies and locally available technology to encrypt and digitally sign organizational E-mail. Office managers will identify individuals responsible for managing the office's organizational E-mail account and ensure time sensitive messages are acted upon promptly. Minimize the number

of users sharing the passwords for office accounts. Per AR 25-11, paragraph 13-3a, routine, unclassified organizational record information may be sent via organizational E–mail in memorandum format. When using E-mail to transmit the record copy of correspondence, E-mail users will state the following in the E-mail note: THIS CORRESPONDENCE IS SENT TO YOU AS ORGANIZATIONAL ELECTRONIC MAIL IAW THE PROVISIONS OF AR 25-11. THIS IS THE OFFICIAL COPY. YOU WILL NOT RECEIVE A PAPER COPY.

f. Users will not represent individual user E-mail messages as a TRADOC position unless the same level of coordination and approval was used in its generation that is used to develop a signed, paper-based TRADOC position.

8. Messaging.

a. The Defense Message System (DMS) is the record messaging system for all organizations in DOD. TRADOC activities that require the use of official organizational messaging will migrate to the DMS. Any message that commits resources, directs action, clarifies official position, or issues official guidance is an organizational message.

b. TRADOC organizations will implement the minimum number of DMS organizational accounts required to accomplish their missions. Since DMS does not support individual accounts, TRADOC organizations will coordinate with their supporting DOIM to establish DMS accounts and to ensure they are correctly listed in the Army Directory Information Tree. Each HQ TRADOC staff section and other TRADOC activities will have at least one unclassified organizational account. Locate the organizational account on one personal computer which will serve as a common user workstation to send/receive DMS messages. Incoming messages are distributed from the common user workstation to appropriate subordinate organizations.

c. TRADOC organizations will coordinate with their supporting DOIM to obtain certificates (Fortezza cards) for their organizational accounts.

d. TRADOC organizations outside Fort Monroe will coordinate with their supporting Installation Operation Center (IOC) to handle their incoming/outgoing classified DMS messages. Each HQ TRADOC staff section with Secret Internet Protocol Router Network (SIPRNET) access will have one classified organizational account available only on the workstation that is connected to the SIPRNET. Those staff sections that do not have SIPRNET access

will use the TRADOC IOC for sending/receiving classified DMS messages.

9. Network access. This paragraph provides commandwide policies specific to managing access to the Internet and military networks.

a. TRADOC activities will maximize the use of DOIM-provided network access services. TRADOC activities will not circumvent or duplicate the Internet access architecture the supporting DOIM operates and maintains. Activities will document local variations or extensions of Army Baseline Services for the provision of services, and any associated reimbursable costs, in a Service Level Agreement with the supporting garrison (that is, DOIM).

b. TRADOC organizations will not establish connections between commercial Internet Service Providers (ISPs) and DOD-operated data networks from the same government IT equipment. TRADOC organizations will access the Internet through the DOD-operated wide area networks. For supported users with special requirements (for example, foreign liaison officers), TRADOC organizations are permitted to use commercial ISPs and subscription services (for example, America Online) through computers and networks that have no network connectivity to military data networks and as locally approved by the supporting DOIM. Do not use TRADOC-owned facilities or equipment to access commercial services unless an official Army contract is in place. Ensure all TRADOC web sites and web-enabled applications are hosted on Army or DOD-operated systems.

c. Ensure electronic material offered or obtained via the Internet is virus free. Ensure virus protection software is used, down to the user level, on any computer system(s) accessing or making electronic material available via the Internet.

d. In accordance with AR 25-1, paragraph 6.3.h, provision of network access is authorized, though not mandated, in personal quarters for key personnel whose duties require immediate response or have a direct bearing on the timely execution of critical actions. Use is restricted to the same authorized uses and IA protections as described throughout this regulation. If such services are provided, TRADOC activities will execute the following measures:

(1) Only government-owned systems may be directly connected to the campus area network.

(2) Install only government-owned software on the system.

(3) Accredit and maintain the system IAW AR 25-2, chapter 5, and DODI 5200.40.

(4) Users must make the equipment in quarters accessible to the system administrator for hardware and software maintenance and IA actions.

e. TRADOC permits the provision of network services for telework. TRADOC Regulation 600-18 prescribes TRADOC's general policies for telework. Government-furnished computer equipment, software, and communications, with appropriate security measures, are required for a recurring telework arrangement that involves use of controlled unclassified information. When IT that is essential to perform the job is unavailable or not securely configured for remote use, the employee will not be approved to telework. Information Management Officers will coordinate provision of network services to teleworkers with the supporting DOIM and IAM.

10. World Wide Web. This paragraph provides commandwide policies specific for managing, operating, and using web sites.

a. As used in this regulation, a homepage is the index or introductory file for a web site. It is designed to be the first file a user visiting a web site accesses. A web site is a collection of files related to a common subject. A web site includes a "homepage" and the linked subordinate information. TRADOC activities will determine their local requirements to produce and maintain web sites and coordinate their establishment with the IMO. Webmasters will coordinate the establishment of new homepages with the TRADOC webmaster (webmaster@monroe.army.mil) and will register public homepages with the Government Information Locator Service (http://sites.defenselink.mil/). Webmasters will coordinate the establishment of new publicly accessible web sites with the supporting PAO, OPSEC officer, and SJA.

b. TRADOC activities will maximize the use of DOIM-provided web services. TRADOC activities will not duplicate web services the supporting DOIM provides unless the DOIM cannot provide the required level of support. Activities will document local variations or extensions of Army Baseline Services for the provision of web services, and any associated reimbursable costs, in a Service Level Agreement with the supporting garrison (for example, DOIM).

c. In accordance with AR 25-2, paragraph 4-20g(15), commanders will conduct annual OPSEC reviews of all organizational web sites and include the results in their annual OPSEC reports.

TRADOC commanders will provide TRADOC DCSINT with these results, and a supplemental report that lists public and private web sites by their Internet Protocol addresses and Uniform Resource Locators, annotated as to whether the site is (1) open to the public, (2) accessible only through AKO authentication, (3) password protected, or (4) authenticated by another specified means.

d. The DCSINT will chair TRADOC's IPWG, which includes the HQ TRADOC CIO, OPSEC officer, PAO, and SJA. The IPWG will meet quarterly, and as required, and will report findings and recommendations to the Command.

e. Webmasters will maintain familiarity with the web site administration policies and procedures defined by DOD and HQDA in memoranda and web sites. Webmasters will implement these procedures as applicable to TRADOC-managed web sites and will ensure the PAO web site content manager is aware of policy and procedure changes. The CIO will conduct periodic visual inspections of TRADOC's public web sites and inform webmasters about findings regarding policy compliance.

f. Webmasters for TRADOC commands, centers, and schools will observe the following policies:

(1) Include a link to the Army homepage and to the TRADOC homepage.

(2) Display a Privacy and Security notice.

(3) Include (or link to) a description of the local mission and organizational structure (do not post names of personnel).

(4) Provide contact information for the webmaster (use an organizational mailbox, for example, webmaster@monroe.army.mil).

(5) Provide disabled web site users access to information that is comparable to the access available to the nondisabled (design guidance available at http://www.section508.gov/).

(6) Do not employ persistent "cookies" or any other automated means to collect personally identifying information on public web sites without the express permission of the user.

g. Before using information retrieved from the WWW for TRADOC's official business, TRADOC general users will ensure such use complies with copyright provisions.

h. Personnel using public web sites to disseminate TRADOC information will coordinate the release of information with PAO (the web site content manager). The PAO will seek assistance as required from supporting OPSEC officers and SJA. Personnel using public web sites to disseminate TRADOC information will provide evidence of reviews as requested by supporting webmasters.

i. Webmasters will ensure web sites within their area of responsibility do not provide methods to bypass access controls (for example, hyperlinks to web pages below password protected web pages).

j. TRADOC activities have the flexibility to use government or commercial sources for webmaster and web authoring support. Select support from the most available, appropriate, and affordable source to adequately perform the mission.

k. Webmasters will monitor the accuracy of links on their web sites. At least monthly, webmasters will review error data in their web site's automated access logs and take action to correct link and document access errors.

l. All links to nongovernment external WWW resources must include a disclaimer that neither DOD nor the local organization endorses the product or organization at the destination, nor does DOD exercise responsibility over the content at the destination.

Appendix A
References

Section I
Required Publications

AR 25-1
Army Knowledge Management and Information Technology Management

AR 25-2
Information Assurance

AR 25-11
Record Communications and the Privacy Communications System

AR 25-400-2
The Army Records Information Management System (ARIMS)

AR 380-5
Department of the Army Information Security Program

Army Website Management and Guidance Memorandum
(http://www.army.mil/webmasters/)

DOD Instruction(DODI) 5200.40
DOD Information Technology Security Certification and Accreditation Process (DITSCAP)

DOD Directive (DODD) 5230.25
Withholding of Unclassified Technical Data from Public Disclosure

DOD 5200.1–R
Information Security Program

DOD 5500.7-R
Joint Ethics Regulation (JER)

DOD 5400.7-R
DOD Freedom of Information Act Program

DOD Web Site Administration Policies and Procedures
(http://www.defenselink.mil/webmasters/policy/dod_web_policy_12071998_with_amendments_and_corrections.html)

TRADOC Regulation 600-18
TRADOC Guidance for the Department of Defense Telework Policy

Section II
Related Publications

AR 25-55
The Department of the Army Freedom of Information Act Program

AR 340-21
The Army Privacy Program

AR 360-1
The Army Public Affairs Program

Glossary

Section I
Abbreviations

AKO	Army Knowledge Online
AR	Army Regulation
CIO	Chief Information Officer
DCSINT	Deputy Chief of Staff for Intelligence
DMS	Defense Message System
DOD	Department of Defense
DOIM	Director of Information Management
DOS	Department of State
E-mail	electronic mail
FOIA	Freedom of Information Act
FOUO	For Official Use Only
HQ	headquarters
HTTP	Hyper Text Transfer Protocol
FTP	file transfer protocol
IA	information assurance
IAM	Information Assurance Manager
IASO	Information Assurance Security Officer
IAW	in accordance with
IMO	Information Management Officer
IOC	Installation Operations Center
IPWG	Information Protection Working Group
ISP	Internet service provider
IT	information technology
JER	Joint Ethics Regulation
MSC	major subordinate command
OPSEC	operations security
PAO	Public Affairs Officer
SBU	Sensitive But Unclassified
SIPRNET	Secret Internet Protocol Router Network
SJA	Staff Judge Advocate
TRADOC	U.S. Army Training and Doctrine Command
TTP	tactics, techniques, and procedures
WWW	World Wide Web

Section II
Terms

Public web site
A web site that is accessible from the Internet and uses no positive access control, for example, user authentication or firewalls, to restrict access to the information posted on the web site. Web site is used to also include any network service that gives a persistent presence to information on the Internet, with

or without a Hyper Text Transfer Protocol (HTTP) front end (for example, FTP site).

Private web site
A web site that screens or challenges users prior to permitting access to the information posted on the site. Private web sites may be connected to an intranet (that is, users are screened from accessing the entire network) or the Internet (that is, users are screened before entry into the specific web site). The term 'web site' also includes any network service that gives a persistent presence to information on the Internet, with or without an HTTP front end (for example, FTP site).

Sensitive information
Any information the loss, misuse, or unauthorized access to, or modification of, which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (The Privacy Act), but which has not been specifically authorized under criteria established by executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Sensitive Information includes information in routine DOD payroll, finance, logistics, and personnel management systems. Examples of sensitive information include, but are not limited to, the following categories:

(1) FOUO – in accordance with DOD 5400.7–R, information that may be withheld from mandatory public disclosure under the FOIA.

(2) Unclassified technical data – Data related to military or dual-use technology that is subject to approval, licenses, or authorization under the Arms Export Control Act and withheld from public disclosure in accordance with DODD 5230.25.

(3) Department of State (DOS) Sensitive But Unclassified (SBU) – Information originating from the DOS that is determined to be SBU under appropriate DOS information security polices.

(4) Foreign Government Information – Information originating from a foreign government that is not classified CONFIDENTIAL or higher but must be protected in accordance with DOD 5200.1–R.

(5) Privacy data – Personal and private information (for example, individual medical information, home address and telephone number, and social security number) as defined in the Privacy Act of 1974. (AR 25-2)

FOR THE COMMANDER:

OFFICIAL:

ANTHONY R. JONES
Lieutenant General, U.S. Army
Deputy Commanding General/
Chief of Staff

/signed/
JANE F. MALISZEWSKI
Colonel, GS
Chief Information Officer